IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF INDIANA
INDIANAPOLIS DIVISION

DARIN JOHNSON and ROBERT WILLEY, on behalf of themselves and all others similarly situated, ***Plaintiffs,*** **v.** **NICE PAK PRODUCTS, INC. and PROFESSIONAL DISPOSABLES INTERNATIONAL, INC.,** ***Defendants***	Case No. 1:23-cv-01734-JMS-CSW

AMENDED CLASS ACTION COMPLAINT

Plaintiffs, Darin Johnson and Robert Willey ("Plaintiffs"), on behalf of themselves and all others similarly situated, bring this action against Defendants Nice-Pak Products, Inc. and Professional Disposables International, Inc. ("Defendants"), and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

NATURE OF THE ACTION

1. This class action arises out of the cyberattack and data breach ("Data Breach") resulting from Defendants' failure to implement reasonable and industry standard data security practices.

2. Defendant Nice-Pak Products, Inc. is a corporation that provides "quality wet wipes" and other healthcare products and/or services to its clients.[1]

[1] https://www.nicepak.com/our-people (last accessed Sep. 13, 2023).

3. Defendant Professional Disposables International, Inc. is a healthcare corporation and affiliate of Defendant Nice-Pak Products, Inc., that provides "products and solutions, educational resources, in-service training, and clinical support" to its clients, which are healthcare providers or similar companies.[2]

4. Plaintiffs' and Class Members' sensitive personal information—which they entrusted to Defendants on the mutual understanding that Defendants would protect it against disclosure—was compromised and unlawfully accessed due to the Data Breach.

5. Defendants collected and maintained certain personally identifiable information of Plaintiffs and the putative Class Members (defined below), who are (or were) employees at one or both of Defendants.

6. The Private Information compromised in the Data Breach included Plaintiffs' and Class Members' full names, addresses, Social Security numbers (collectively, "personally identifiable information" or "Private Information") and medical and health insurance information, which is protected health information ("PHI", and collectively with Private Information, "Private Information" or "PII") as defined by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA").

7. The Private Information compromised in the Data Breach was exfiltrated by cyber-criminals and remains in the hands of those cyber-criminals who target Private Information for its value to identity thieves.

8. As a result of the Data Breach, Plaintiffs and potentially thousands of Class Members, suffered concrete injury in fact including, but not limited to: (i) invasion of privacy; (ii) theft of Private Information; (iii) lost or diminished value of Private Information; (iv) lost time and

[2] https://pdihc.com/ (last accessed Sep. 13, 2023).

opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their Private Information, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the Private Information.

9. The Data Breach was a direct result of Defendants' failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect their employees' Private Information from a foreseeable and preventable cyber-attack.

10. Defendants maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendants' computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendants, and thus, Defendants were on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

11. Defendants disregarded the rights of Plaintiffs and Class Members by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure their data systems were protected against unauthorized intrusions; failing to disclose that they did not have adequately robust computer systems and security practices to safeguard Class Members' Private Information; failing to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiffs and Class Members prompt and accurate notice of the Data Breach.

12. Plaintiffs' and Class Members' identities are now at risk because of Defendants' negligent conduct because the Private Information that Defendants collected and maintained is now in the hands of data thieves.

13. Armed with the Private Information accessed in the Data Breach, data thieves have already engaged in identity theft and fraud (including the fraud suffered by Plaintiffs described below), and can in the future commit a variety of crimes including, *e.g.*, opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

14. As a result of the Data Breach, Plaintiffs and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

15. Plaintiffs and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

16. Plaintiffs bring this class action lawsuit on behalf of those similarly situated to address Defendants' inadequate safeguarding of Class Members' Private Information that it collected and maintained, and for failing to provide timely and adequate notice to Plaintiffs and other Class Members that their information had been subject to the unauthorized access by an unknown third party and precisely what specific type of information was accessed.

17. Through this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was accessed during

the Data Breach.

18. Plaintiffs seek remedies including, but not limited to, compensatory damages and injunctive relief including improvements to Defendants' data security systems, future annual audits, and adequate credit monitoring services funded by Defendants.

19. Accordingly, Plaintiffs bring this action against Defendants seeking redress for their unlawful conduct.

PARTIES

20. Plaintiff Darin Johnson is a resident and citizen of Indianapolis, Indiana. He is a former employee of Defendant Nice-Pak Products, Inc. and worked there from approximately 2009 to 2012. As a condition of Plaintiff Johnson's employment at Nice-Pak Products, Inc., he was required to provide his Private Information to Defendant Nice-Pak Products, Inc.

21. Plaintiff Johnson received the Notice Letter directly from Defendant Nice-Pak Products, Inc., via U.S. mail, dated August 14, 2023 (the "Notice Letter"). If Mr. Johnson had known that Defendants would not adequately protect his Private Information, he would not have entrusted Defendants with his Private Information or allowed Defendants to maintain this sensitive Private Information.

22. Plaintiff Robert Willey is a resident and citizen of Nanuet, New York. He is a former employee of Defendant Nice-Pak Products, Inc. and worked there from approximately 2016 to 2021. As a condition of Plaintiffs' employment at Nice-Pak Products, Inc., he was required to provide his Private Information to Defendant Nice-Pak Products, Inc..

23. Plaintiff Willey received the Notice Letter directly from Defendant Nice-Pak Products, Inc., via U.S. mail, dated August 14, 2023. If Mr. Willey had known that Defendants would not adequately protect his Private Information, he would not have entrusted Defendants

with his Private Information or allowed Defendants to maintain this sensitive Private Information.

24. Defendant Nice-Pak Products, Inc. is a corporation duly formed and existing under the laws of the State of New York with a principal place of business in Rockland County, New York.

25. Defendant Professional Disposables International, Inc. is a corporation duly formed and existing under the laws of the State of Delaware with a principal place of business in Bergen County, New Jersey. Defendant Professional Disposable International, Inc. is an affiliate of Defendant Nice-Pak Products, Inc.

JURISDICTION AND VENUE

26. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount in controversy exceeds the sum of $5,000,000 exclusive of interest and costs, there are more than 100 putative class members, and minimal diversity exists because many putative class members including Plaintiffs are citizens of a different state than Defendants. This Court also has supplemental jurisdiction pursuant to 28 U.S.C. § 1367(a) because all claims alleged herein form part of the same case or controversy.

27. This Court has personal jurisdiction over Defendants because, personally or through their agents, Defendants operate, conduct, engage in, or carry on a business in Indiana and committed tortious acts in Indiana.

28. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the events and omissions giving rise to Plaintiffs' claims occurred in this district.

BACKGROUND FACTS

A. Defendants' Businesses

29. Nice-Pak Products, Inc. is a corporation that provides "quality wet wipes" and other

healthcare products and/or services to its clients.[3]

30. Defendant Professional Disposables International, Inc. is a healthcare corporation and affiliate of Defendant Nice-Pak Products, Inc., that provides "products and solutions, educational resources, in-service training, and clinical support" to its clients, which are healthcare providers or similar companies.[4]

31. Upon information and belief, in the course of collecting Private Information from employees, including Plaintiff, Defendants promised to provide confidentiality and adequate security for employee data through their applicable privacy policy and through other disclosures in compliance with statutory privacy requirements.

32. Indeed, Defendant Nice-Pak Products, Inc.'s Privacy Policy provides that: "[w]e are committed to the protection of your information. We may store Personal Data or such information may be stored by third parties to whom we have transferred it in accordance with this Privacy Policy. We take what we believe to be reasonable steps to protect the Personal Data collected via the Site from loss, misuse, unauthorized access, inadvertent disclosure, alteration, and destruction."[5]

33. Similarly, Defendant Professional Disposables International, Inc.'s Privacy Policy provides that: "[w]e are committed to the protection of your information. We may store Personal Data or such information may be stored by third parties to whom we have transferred it in accordance with this Privacy Policy. We take what we believe to be reasonable steps to protect the Personal Data collected via the Site from loss, misuse, unauthorized access, inadvertent disclosure,

[3] https://www.nicepak.com/our-people (last accessed Sep. 13, 2023).
[4] https://pdihc.com/ (last accessed Sep. 13, 2023).
[5] https://www.nicepak.com/privacy-policy (last accessed Sep. 13, 2023).

alteration, and destruction."[6]

34. Plaintiffs and the Class Members, as former and current employees at one or both of Defendants, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Employees, in general, demand security to safeguard their Private Information, especially when Social Security numbers and other sensitive Private Information is involved.

35. In the course of their employment relationship, employees, including Plaintiffs and Class Members, provided one or both of Defendants with at least the following Private Information:

a. names;

b. Social Security numbers; and

c. Addresses.

36. Defendants had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

The Data Breach

37. On or about August 14, 2023, Defendant Nice-Pak Products, Inc., on behalf of Defendants, began sending Plaintiffs and other victims of the Data Breach an untitled letter (the "Notice Letter"), informing them that:

> Nice Pak Products, Inc. and Professional Disposables International, Inc. understand the importance of protecting information. We are writing to inform you that we recently identified and addressed a data security incident involving your information. This letter explains the incident, the measures we have taken, and steps you may consider taking in response.

[6] https://pdihc.com/privacy/ (last accessed Sep. 13, 2023).

What Happened?
On June 15, 2023, we identified unusual activity on certain devices in our network. We immediately implemented our response protocols, took measures to contain the activity, and launched an investigation. A cybersecurity firm also was engaged. We notified law enforcement and are supporting its investigation.

The evidence showed that between May 28, 2023 and June 15, 2023, an unauthorized actor viewed and obtained files stored on certain servers in our network. We conducted a careful review of the files and, on July 24, 2023, determined that one or more of the files contained your information.

What Information Was Involved?
The files contained your name, address, Social Security number, health plan member number, and for a small number of individuals, your health savings account number.[7]

38. Omitted from the Notice Letter were the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure such a breach does not occur again. To date, these omitted details have not been explained or clarified to Plaintiffs and Class Members, who retain a vested interest in ensuring that their Private Information remains protected.

39. Upon information and belief, Defendants share a computer network(s), on which Plaintiffs' and Class Member's Private Information was stored on at the time of the Data Breach.

40. Upon information and belief, the cyberattack was targeted at Defendants, due to their statuses as employers that collect, create, and maintain Private Information on their computer networks and/or systems.

41. Upon information and belief, Plaintiffs' and Class Members' Private Information was, in fact, involved in the Data Breach.

42. The files, containing Plaintiffs' and Class Members' Private Information and stolen from Defendants, included the following: names, addresses, Social Security numbers, health plan

[7] The "Notice Letter". A sample copy is available at https://www.doj.nh.gov/consumer/security-breaches/documents/nice-pak-products-20230814.pdf (last accessed Sep. 13, 2023).

member numbers, and health saving account numbers.[8]

43. Because of this targeted cyberattack, data thieves were able to gain access to and obtain data from Defendants that included the Private Information of Plaintiffs and Class Members.

44. As evidenced by the Data Breach's occurrence, the Private Information contained in Defendants' networks was not encrypted. Had the information been properly encrypted, the data thieves would have exfiltrated only unintelligible data.

45. Plaintiffs' Private Information was accessed and stolen in the Data Breach and Plaintiffs believe their stolen Private Information is currently available for sale on the dark web because that is the *modus operandi* of cybercriminals.

46. Due to the actual and imminent risk of identity theft as a result of the Data Breach, Plaintiffs and Class Members must, as Defendants' Notice Letter encourages, monitor their financial accounts for many years to mitigate the risk of identity theft.[9]

47. In the Notice Letter, Defendants make an offer of 12 months of identity monitoring services. This is wholly inadequate to compensate Plaintiffs and Class Members as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft, medical and financial fraud, and it entirely fails to provide sufficient compensation for the unauthorized release and disclosure of Plaintiffs' and Class Members' Private Information.

48. That Defendants are encouraging their current and former employees to enroll in credit monitoring and identity theft restoration services is an acknowledgment that the impacted

[8] *Id.*
[9] *Id.*

individuals' Private Information *was* accessed, thereby subjecting Plaintiffs and Class Members to a substantial and imminent threat of fraud and identity theft.

49. Defendants had obligations created by contract, state and federal law, common law, and industry standards to keep Plaintiffs' and Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

B. Defendants Failed to Safeguard Employee PII

50. Defendants collect and maintain employee PII in their computer systems as a condition of employment.

51. In collecting and maintaining the PII, Defendants agreed they would safeguard the data according to state and federal law and their internal policies, including those above.

52. Despite those promises, Defendants lost control over their employees' PII.

53. In May 2023, hackers bypassed Defendants' cybersecurity undetected and accessed their employees' PII. Defendants did not detect the hack when it happened, nor would they for two weeks, meaning Defendants did not have the means to prevent, detect, or stop data breaches before hackers could access and steal PII.

54. Defendants detected the breach on June 15, 2023. As a result, cybercriminals could access and pilfer the PII belonging to Defendants' employees from May 28, 2023 until June 15, 2023—two weeks after the breach started.

55. Thus, cybercriminals accessed and stole employees' PII, including their names and Social Security numbers, health insurance plan information, and health savings account information. Indeed, Defendants refer to the Data Breach as the "Health Plan Incident."[10]

56. Defendants did not notify their employees that hackers had stolen their information,

[10] https://www.nicepak.com/home; https://www.nicepak.com/media/wysiwyg/nicepak/Nice-Pak_Notice-of-health-plan-incident_v2.pdf (last accessed August 23, 2023).

nor would it until August 2023.

57. By July 24, 2023 Defendants concluded their "investigation" and notified their employees about the breach.

58. Defendants are warning their employees and their families to monitor their credit scores and enroll in credit monitoring, thus recognizing that employees should protect themselves from identity theft following the Data Breach.

59. On information and belief, Defendants failed to adequately train their employees on reasonable cybersecurity protocols or implement reasonable security measures, causing them to lose control over employee PII. Defendants' negligence is evidenced by their failure to prevent the Data Breach and stop cybercriminals from accessing PII. Further, the Breach Notice makes clear that Defendants cannot, or will not, determine the full scope of the Data Breach, as they have been unable to determine exactly what information was stolen and when.

C. Plaintiffs' Experiences

Plaintiff Johnson's Experience

60. Prior to the Data Breach, Plaintiff Johnson was employed at Nice-Pak Products, Inc. from approximately 2009 to 2012.

61. In the course of enrolling in employment with Nice-Pak Products, Inc. and as a condition of employment, he was required to supply Nice-Pak Products, Inc. with his Private Information—including, but not limited to his name, address, and Social Security number.

62. Plaintiff Johnson is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

63. At the time of the Data Breach—from May 28, 2023 through June 15, 2023—

Defendants retained Plaintiff's Private Information in their system, despite no longer maintaining an employment relationship with Plaintiff for approximately two years.

64. Plaintiff Johnson received the Notice Letter, by U.S. mail, directly from Defendant Nice-Pak Products, Inc., dated August 14, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his full name, address, Social Security number, health plan member number, and health savings account number. Plaintiff has spent significant time remedying the breach—time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

65. Upon receiving the Notice Letter from Defendant Nice-Pak Products, Inc., Plaintiff Johnson has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft insurance offered by Defendant, and contacting financial institutions to ensure his accounts are secure.

66. Subsequent to the Data Breach, Plaintiff Johnson has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

67. Plaintiff Johnson additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant Nice-Pak Products, Inc. was the requirement that it adequately safeguard his Private Information and that it would delete or destroy his Private Information after Defendants were no longer required to retain it. Plaintiff Johnson would not have worked for Defendant Nice-Pak Products, Inc. had Nice-Pak Products, Inc. disclosed that it lacked data security practices adequate to safeguard Private Information.

68. Plaintiff Johnson further suffered actual injury in the form of damages and diminution in the value of his Private Information —a form of intangible property that he entrusted to Defendant Nice-Pak Products, Inc. for the purpose of employment, which was compromised by the Data Breach.

69. Plaintiff Johnson also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

70. Plaintiff Johnson has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

71. Plaintiff Johnson has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff Willey's Experience

72. Prior to the Data Breach, Plaintiff Willey was employed at Nice-Pak Products, Inc. from approximately 2016 to 2021.

73. In the course of enrolling in employment with Nice-Pak Products, Inc. and as a condition of employment, he was required to supply Nice-Pak Products, Inc. with his Private

Information—including, but not limited to his name, address, and Social Security number.

74. Plaintiff Willey is very careful about sharing his sensitive Private Information. Plaintiff stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source.

75. At the time of the Data Breach—from May 28, 2023 through June 15, 2023—Defendants retained Plaintiff's Private Information in their system, despite no longer maintaining an employment relationship with Plaintiff for approximately two years.

76. Plaintiff Willey received the Notice Letter, by U.S. mail, directly from Defendant Nice-Pak Products, Inc., dated August 14, 2023. According to the Notice Letter, Plaintiff's Private Information was improperly accessed and obtained by unauthorized third parties, including his full name, address, Social Security number, health plan member number, and health savings account number. Plaintiff has spent significant time remedying the breach—time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

77. Upon receiving the Notice Letter from Defendant Nice-Pak Products, Inc., Plaintiff Willey has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter, signing up for the credit monitoring and identity theft insurance offered by Defendant, and contacting financial institutions to ensure his accounts are secure.

78. Subsequent to the Data Breach, Plaintiff Willey has suffered numerous, substantial injuries including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual

consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

79. Plaintiff Willey additionally suffered actual injury and damages as a result of the Data Breach. Implied in his employment contract with Defendant Nice-Pak Products, Inc. was the requirement that it adequately safeguard his Private Information and that it would delete or destroy his Private Information after Defendants were no longer required to retain it. Plaintiff Willey would not have worked for Defendant Nice-Pak Products, Inc. had Nice-Pak Products, Inc. disclosed that it lacked data security practices adequate to safeguard Private Information.

80. Plaintiff Willey further suffered actual injury in the form of damages and diminution in the value of his Private Information —a form of intangible property that he entrusted to Defendant Nice-Pak Products, Inc. for the purpose of employment, which was compromised by the Data Breach.

81. Plaintiff Willey also suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy, especially his Social Security number, being in the hands of criminals.

82. Plaintiff Willey has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his stolen Private Information being placed in the hands of unauthorized third parties and possibly criminals.

83. Plaintiff Willey has a continuing interest in ensuring that his Private Information,

which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

D. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

84. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendant.

85. As a result of Defendants' failure to prevent the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

a. The loss of the opportunity to control how their PII is used;

b. The diminution in value of their PII;

c. The compromise and continuing publication of their PII;

d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;

e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

f. Delay in receipt of tax refund monies;

g. Unauthorized use of stolen PII; and

h. The continued risk to their PII, which remains in the possession of Defendants and is subject to further breaches so long as Defendants fail to undertake the appropriate measures to protect the PII in their possession.

86. Stolen PII is one of the most valuable commodities on the criminal information black market. According to Experian, a credit-monitoring service, stolen PII can be worth up to

$1,000.00 depending on the type of information obtained.

87. The value of Plaintiffs and the proposed Class's PII on the black market is considerable. Stolen PII trades on the black market for years, and criminals frequently post stolen private information openly and directly on various "dark web" internet websites, making the information publicly available, for a substantial fee of course.

88. It can take victims years to spot identity or PII theft, giving criminals plenty of time to use that information for cash.

89. Cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

90. One such example of criminals piecing together bits and pieces of compromised PII for profit is the development of "Fullz" packages.[11]

91. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

92. The development of "Fullz" packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs and the proposed Class's phone

[11] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-](https://krebsonsecuritv.eom/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-finn/ (last visited on May 26, 2023).

numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cyber-criminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over. That is exactly what is happening to Plaintiffs and members of the proposed Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiffs and other members of the proposed Class's stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

93. The existence and prevalence of "Fullz" packages means that the PII stolen from the data breach can easily be linked to the unregulated data (like driver's license numbers) of Plaintiffs and the other Class Members.

94. Thus, even if certain information (such as driver's license numbers) was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

95. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals (like illegal and scam telemarketers).

96. Defendants disclosed the PII of Plaintiffs and members of the proposed Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiffs and members of the proposed Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

97. Defendants' failure to properly notify Plaintiffs and members of the proposed Class of the Data Breach exacerbated Plaintiffs and members of the proposed Class's injury by depriving

them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach.

E. Defendants Failed to Adhere to FTC guidelines.

98. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendant, should employ to protect against the unlawful exposure of PII.

99. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

a. protect the personal customer information that they keep;

b. properly dispose of personal information that is no longer needed;

c. encrypt information stored on computer networks;

d. understand their network's vulnerabilities; and

e. implement policies to correct security problems.

100. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

101. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

102. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer data, treating the failure to employ reasonable and

appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

103. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to employees' PII constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

F. Defendants Failed to Adhere to Industry Standards.

104. As noted above, experts studying cyber security routinely identify entities in possession of Private Information as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

105. Several best practices have been identified that a minimum should be implemented by employers in possession of Private Information, like Defendants, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data and limiting which employees can access sensitive data. Defendants failed to follow these industry best practices, including a failure to implement multi-factor authentication.

106. Other best cybersecurity practices that are standard for employers include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points. Defendants failed to follow these cybersecurity best practices, including failure to train staff.

107. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

108. These foregoing frameworks are existing and applicable industry standards for an employer's obligations to provide adequate data security for its employees. Upon information and belief, Defendants failed to comply with at least one—or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

CLASS ACTION ALLEGATIONS

109. Plaintiffs incorporate by reference all other paragraphs of this Complaint as if fully set forth herein.

110. Plaintiffs bring this nationwide class action on behalf of themselves and all other persons similarly situated ("the Nationwide Class") pursuant to Rule 23(a) of the Federal Rules of Civil Procedure, and Fed. R. Civ. P. 23(b)(3).

111. Plaintiffs propose the following Class definition (the "Nationwide Class"), subject to amendment based on information obtained through discovery:

> **All persons residing in the United States whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendants in August 2023, including all persons who received the Notice Letter.**

112. In addition, or in the alternative, Plaintiffs propose the following state class ("New York Class") (together with the Nationwide Class, "the Class"):

> **All New York citizens whose PII was accessed and/or acquired by an unauthorized party as a result of the Data Breach reported by Defendants in**

August 2023, including all persons who received the Notice Letter.

113. Excluded from the Classes are Defendants' officers, directors, and employees; any entity in which Defendants has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and members of their staff.

114. Plaintiffs reserve the right to amend the definition of the Class and/or New York Class or add a class or subclass if further information and discovery indicate that the definition of the Class should be narrowed, expanded, or otherwise modified.

115. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of Class Members' claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims for each Class Member.

116. This action satisfies the requirements for a class action under Fed. R. Civ. P. 23(a)(1)-(3) and Fed. R. Civ. P. 23(b)(2), including requirements of numerosity, commonality, typicality, adequacy, predominance, and superiority.

117. **Numerosity, Fed. R. Civ. P. 23(a)(1):** The members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the PII of approximately 12,996 current and former customers of Defendants was compromised in the Data Breach. Such information is readily ascertainable from Defendants' records.

118. **Commonality, Fed. R. Civ. P. 23(a)(2):** There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendants unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' PII;

b. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations including, *e.g.*, the FTC Act;

d. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether computer hackers obtained Class Members' PII in the Data Breach;

f. Whether Defendants knew or should have known that their data security systems and monitoring processes were deficient;

g. Whether Plaintiffs and the Class Members suffered legally cognizable damages as a result of Defendants' misconduct;

h. Whether Defendants breached the covenant of good faith and fair dealing implied in their contracts with Plaintiffs and Class Members;

i. Whether Defendants' acts violated Kentucky law, and;

j. Whether Plaintiffs and the Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

119. **Typicality, Fed. R. Civ. P. 23(a)(3):** The claims or defenses of Plaintiffs are typical of the claims or defenses of the proposed Class because Plaintiffs' claims are based upon the same legal theories and same violations of law. Plaintiffs' claims are typical of those of other Class

Members because Plaintiffs' PII, like that of every other Class Member, was compromised in the Data Breach.

120. **Adequacy, Fed. R. Civ. P. 23(a)(4):** Plaintiffs will fairly and adequately represent and protect the interests of the members of the Class. Plaintiffs' Counsel are competent and experienced in litigating class actions.

121. **Predominance, Fed. R. Civ. P. 23(b)(3):** Defendants have engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data—PII—was stored on the same computer systems and unlawfully exposed in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

122. **Superiority, Fed. R. Civ. P. 23(b)(3):** A class action is a superior method for the fair and efficient adjudication of this controversy because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy, and joinder of the Class Members is otherwise impracticable. Class treatment presents a superior mechanism for fairly resolving similar issues and claims without repetitious and wasteful litigation for many reasons, including the following:

a. It would be a substantial hardship for most individual members of the Class if they were forced to prosecute individual actions. Many members of the Class are not in the position to incur the expense and hardship of retaining their own counsel to prosecute individual actions, which in any event might cause inconsistent results.

b. When the liability of Defendants has been adjudicated, the Court will be able to

determine the claims of all members of the Class. This will promote global relief and judicial efficiency in that the liability of Defendants to all Class Members, in terms of money damages due and in terms of equitable relief, can be determined in this single proceeding rather than in multiple, individual proceedings where there will be a risk of inconsistent and varying results.

c. A class action will permit an orderly and expeditious administration of the Class claims, foster economies of time, effort, and expense, and ensure uniformity of decisions. If Class Members are forced to bring individual suits, the transactional costs, including those incurred by Defendant, will increase dramatically, and the courts will be clogged with a multiplicity of lawsuits concerning the very same subject matter, with identical fact patterns and the same legal issues. A class action will promote a global resolution and will promote uniformity of relief as to the Class Members and as to Defendant.

d. This lawsuit presents no difficulties that would impede its management by the Court as a class action. The class certification issues can be easily determined because the Class includes only Nice Pak's customers, the legal and factual issues are narrow and easily defined, and the Class membership is limited. The Class does not contain so many persons that would make the Class notice procedures unworkable or overly expensive. The identity of the Class Members can be identified from Defendants' records, such that direct notice to the Class Members would be appropriate.

123. In addition, Defendants have acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are

appropriate on a class-wide basis.

124. Likewise, particular issues are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendants failed to timely and adequately notify the public of the Data Breach;

b. Whether Defendants owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, and safeguarding their PII;

c. Whether Defendants' security measures to protect their data systems were reasonable in light of best practices recommended by data security experts;

d. Whether Defendants' failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendants failed to take commercially reasonable steps to safeguard consumer PII; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

125. Finally, all members of the proposed Class are readily ascertainable. Defendants have access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Class)

126. Plaintiffs reallege all previous paragraphs as if fully set forth below.

127. Plaintiffs and members of the Class entrusted their PII to Defendant. Defendants owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PII in their care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

128. Defendants owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendants' failure to adequately safeguard their PII in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PII—just like the Data Breach that ultimately came to pass. Defendants acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PII by disclosing and providing access to this information to third parties and by failing to properly supervise both the way the PII was stored, used, and exchanged, and those in their employ who were responsible for making that happen.

129. Defendants owed to Plaintiffs and members of the Class a duty to notify them within a reasonable timeframe of any breach to the security of their PII. Defendants also owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the scope, nature, and occurrence of the Data Breach. This duty is required and necessary for Plaintiffs and members of the Class to take appropriate measures to protect their PII, to be vigilant in the face of an increased risk of harm, and to take other necessary steps to mitigate the harm caused by the Data Breach.

130. Defendants owed these duties to Plaintiffs and members of the Class because they are members of a well-defined, foreseeable, and probable class of individuals whom Defendants knew or should have known would suffer injury-in-fact from Defendants' inadequate security

protocols. Defendants actively sought and obtained Plaintiffs' and members of the Class's personal information and PII.

131. The risk that unauthorized persons would attempt to gain access to the PII and misuse it was foreseeable. Given that Defendants holds vast amounts of PII, it was inevitable that unauthorized individuals would attempt to access Defendants' databases containing the PII—whether by malware or otherwise.

132. PII is highly valuable, and Defendants knew, or should have known, the risk in obtaining, using, handling, emailing, and storing the PII of Plaintiffs and members of the Class's and the importance of exercising reasonable care in handling it.

133. Defendants breached their duties by failing to exercise reasonable care in supervising their agents, contractors, vendors, and suppliers, and in handling and securing the personal information and PII of Plaintiffs and members of the Class which actually and proximately caused the Data Breach and Plaintiffs and members of the Class's injury. Defendants further breached their duties by failing to provide reasonably timely notice of the Data Breach to Plaintiffs and members of the Class, which actually and proximately caused and exacerbated the harm from the Data Breach and Plaintiffs and members of the Class's injuries-in-fact. As a direct and traceable result of Defendants' negligence and/or negligent supervision, Plaintiffs and members of the Class have suffered or will suffer damages, including monetary damages, increased risk of future harm, embarrassment, humiliation, frustration, and emotional distress.

134. Defendants' breach of their common-law duties to exercise reasonable care and their failures and negligence actually and proximately caused Plaintiffs and members of the Class actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PII by criminals, improper disclosure of their PII, lost benefit of their bargain, lost value of their PII, and

lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendants' negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

COUNT II
NEGLIGENCE PER SE
(On Behalf of Plaintiffs and the Class)

135. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

136. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's PII.

137. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect customers or, in this case, employees' PII. The FTC publications and orders promulgated pursuant to the FTC Act also form part of the basis of Defendants' duty to protect Plaintiffs and the members of the Class's sensitive PII.

138. Defendants violated their duty under Section 5 of the FTC Act by failing to use reasonable measures to protect their employees' PII and not complying with applicable industry standards as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII Defendants had collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to their employees in the event of a breach, which ultimately came to pass.

139. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive

practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

140. Defendants had a duty to Plaintiffs and the members of the Class to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs and the Class's PII.

141. Defendants breached their respective duties to Plaintiffs and members of the Class under the FTC Act by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and members of the Class's PII.

142. Defendants' violation of Section 5 of the FTC Act and their failure to comply with applicable laws and regulations constitutes negligence per se.

143. But for Defendants' wrongful and negligent breach of their duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

144. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendants' breach of their duties. Defendants knew or should have known that Defendants was failing to meet their duties and that their breach would cause Plaintiffs and members of the Class to suffer the foreseeable harms associated with the exposure of their PII.

145. Had Plaintiffs and members of the Class known that Defendants did not adequately protect their PII, Plaintiffs and members of the Class would not have entrusted Defendants with their PII.

146. As a direct and proximate result of Defendants' negligence per se, Plaintiffs and members of the Class have suffered harm, including loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of PII; unreimbursed losses relating to fraudulent charges; losses relating to exceeding credit and debit card limits and balances; harm resulting from damaged credit scores

and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT III
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Class)

147. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

148. Defendants offered to employ Plaintiffs and members of the Class in exchange for their PII.

149. In turn, Defendants agreed it would not disclose the PII it collects to unauthorized persons. Defendants also promised to safeguard employee PII.

150. Plaintiffs and the members of the Class accepted Defendants' offer by providing PII to Defendants in exchange for employment with Defendant.

151. Implicit in the parties' agreement was that Defendants would provide Plaintiffs and members of the Class with prompt and adequate notice of all unauthorized access and/or theft of their PII.

152. Plaintiffs and the members of the Class would not have entrusted their PII to Defendants in the absence of such agreement with Defendant.

153. Defendants materially breached the contract(s) it had entered with Plaintiffs and members of the Class by failing to safeguard such information and failing to notify them promptly of the intrusion into their computer systems that compromised such information. Defendants further breached the implied contracts with Plaintiffs and members of the Class by:

a. Failing to properly safeguard and protect Plaintiffs and members of the Class's PII;

b. Failing to comply with industry standards as well as legal obligations that are necessarily incorporated into the parties' agreement; and

c. Failing to ensure the confidentiality and integrity of electronic PII that Defendants created, received, maintained, and transmitted.

154. The damages sustained by Plaintiffs and members of the Class as described above were the direct and proximate result of Defendants' material breaches of their agreement(s).

155. Plaintiffs and members of the Class have performed as required under the relevant agreements, or such performance was waived by the conduct of Defendant.

156. The covenant of good faith and fair dealing is an element of every contract. All such contracts impose upon each party a duty of good faith and fair dealing. The parties must act with honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection with executing contracts and discharging performance and other duties according to their terms, means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a contract are mutually obligated to comply with the substance of their contract in addition to their form.

157. Subterfuge and evasion violate the obligation of good faith in performance even when an actor believes their conduct to be justified. Bad faith may be overt or may consist of inaction, and fair dealing may require more than honesty.

158. Defendants failed to advise Plaintiffs and members of the Class of the Data Breach promptly and sufficiently.

159. In these and other ways, Defendants violated their duty of good faith and fair dealing.

160. Plaintiffs and members of the Class have sustained damages because of Defendants' breaches of their agreement, including breaches thereof through violations of the covenant of good faith and fair dealing.

COUNT IV
UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Class)

161. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

162. This claim is pleaded in the alternative to the breach of implied contractual duty claim.

163. Plaintiffs and members of the Class conferred a benefit upon Defendants in the form of services through employment.

164. Defendants appreciated or had knowledge of the benefits conferred upon itself by Plaintiffs and members of the Class. Defendants also benefited from the receipt of Plaintiffs and members of the Class's PII, as this was used to facilitate their employment.

165. Under principals of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiffs and the proposed Class's services and their PII because Defendants failed to adequately protect their PII. Plaintiffs and the proposed Class would not have provided their PII or worked for Defendants at the payrates they did had they known Defendants would not adequately protect their PII.

166. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiffs and members of the Class all unlawful or inequitable proceeds received by it because of their misconduct and Data Breach.

COUNT V
BAILMENT
(On Behalf of Plaintiffs and the Class)

167. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

168. Plaintiffs, the Class Members, and Defendants contemplated a mutual benefit

bailment when the Plaintiffs and putative members of the Class transmitted their PII to Defendants solely for the purpose of obtaining employment.

169. Plaintiffs and the Class entrusted their PII to Defendants for a specific purpose—to obtain employment—with an implied contract that the trust was to be faithfully executed, and the PII was to be accounted for when the special purpose was accomplished.

170. Defendants accepted the Plaintiffs' and the Class's PII for the specific purpose of employment.

171. Defendants were duty bound under the law to exercise ordinary care and diligence in safeguarding Plaintiffs' and the Class's PII.

172. Plaintiffs' and the Class's PII was used for a different purpose than the Plaintiff and the Class intended, for a longer time period and/or in a different manner or place than Plaintiff and the Class intended.

173. As set forth in the preceding paragraphs, Plaintiffs and the Class Members were damaged thereby.

COUNT VI
VIOLATION OF THE NEW YORK DECEPTIVE TRADE PRACTICES ACT ("GBL")
(New York Gen. Bus. Law § 349)
(On Behalf of Plaintiff Willey and New York Class)

174. Plaintiff Willey ("Plaintiff" for the purposes of this Count) re-alleges and incorporates the above allegations, as if fully set forth herein, and brings this claim on behalf of himself and the New York Class (the "Class" for the purposes of this count).

175. Defendants engaged in deceptive, unfair, and unlawful trade acts or practices in the conduct of trade or commerce and furnishing of services, in violation of N.Y. Gen. Bus. Law § 349(a), including but not limited to the following:

a. Misrepresenting material facts to Plaintiff and the Class by representing that they

would maintain adequate data privacy and security practices and procedures to safeguard Class Members' PII from unauthorized disclosure, release, data breaches, and theft;

b. Misrepresenting material facts to Plaintiff and the Class by representing that they did and would comply with the requirements of federal and state laws pertaining to the privacy and security of Class Member's PII;

c. Omitting, suppressing, and/or concealing material facts of the inadequacy of their privacy and security protections for Class Members' PII;

d. Engaging in deceptive, unfair, and unlawful trade acts or practices by failing to maintain the privacy and security of Class Members' PII, in violation of duties imposed by and public policies reflected in applicable federal and state laws; and,

e. Engaging in deceptive, unfair and unlawful trade acts or practices by failing to disclose the Data Breach to the Class in a timely and accurate manner, contrary to the duties imposed by N.Y. Gen. Bus. Law § 899-aa(2).

176. Defendants knew or should have known that their network and data security practices were inadequate to safeguard the Class Members' Private Information entrusted to it, and that risk of a data breach or theft was highly likely.

177. Defendants should have disclosed this information because Defendants were in a superior position to know the true facts related to the defective data security.

178. Defendants' failure to disclose constitutes false and misleading representations, which have the capacity, tendency, and effect of deceiving or misleading consumers (including Plaintiffs and Class Members) regarding the security of Defendants' network and aggregation of Private Information.

179. The representations upon which current and former employees (including Plaintiff and Class Members) relied were material representations (e.g., as to Defendants' adequate protection of Private Information), and current and former employees (including Plaintiff and Class Members) relied on those representations to their detriment.

180. Defendants' conduct is unconscionable, deceptive, and unfair, as it is likely to, and did, mislead consumers acting reasonably under the circumstances. As a direct and proximate result of Defendants' conduct, Plaintiff and other Class Members have been harmed, in that they were not timely notified of the Data Breach, which resulted in profound vulnerability to their personal information and other financial accounts.

181. Defendants knew or should have known that their computer systems and data security practices were inadequate to safeguard Class Members' Private Information and that the risk of a data security incident was high.

182. Defendants' acts, practices, and omissions were done in the course of Defendants' business of furnishing employment benefit services to consumers in the State of New York. 167.

183. As a direct and proximate result of Defendants' unconscionable, unfair, and deceptive acts and omissions, Plaintiff's and Class Members' Private Information was disclosed to third parties without authorization, causing and will continue to cause Plaintiff and Class Members damages.

184. Plaintiff and Class Members were injured because:

a. Plaintiff and Class Members would not have accepted employment at Defendants had they known the true nature and character of Defendants' data security practices;

b. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of promises that Defendants would keep their

information reasonably secure, and

c. Plaintiff and Class Members would not have entrusted their Private Information to Defendants in the absence of the promise to monitor their computer systems and networks to ensure that they adopted reasonable data security measures.

185. As a direct and proximate result of Defendants' multiple, separate violations of GBL §349, Plaintiff and the Class Members suffered damages including, but not limited to: (i) invasion of privacy; (ii) theft of PII; (iii) lost or diminished value of PII; (iv) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (v) loss of benefit of the bargain; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; and (vii) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

186. As a result, Plaintiff and the Class Members have been damaged in an amount to be proven at trial.

187. Plaintiff brings this action on behalf of himself and Class Members for the relief requested above and for the public benefit to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiff, Class Members and the public from Defendants' unfair, deceptive, and unlawful practices. Defendants' wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

188. Plaintiff and Class Members seek relief under N.Y. Gen. Bus. Law § 349(h),

including, but not limited to, actual damages, treble damages, statutory damages, injunctive relief, and/or attorney's fees and costs.

189. On behalf of himself and other members of the Class, Plaintiff seeks to enjoin the unlawful acts and practices described herein, to recover his actual damages or fifty dollars, whichever is greater, three times actual damages, and reasonable attorneys' fees.

190. Also as a direct result of Defendants' violation of GBL § 349, Plaintiff and the Class Members are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendants to: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

PRAYER FOR RELIEF

Plaintiffs and members of the Class demand a jury trial on all claims so triable and request that the Court enter an order:

A. Certifying this case as a class action on behalf of Plaintiffs and the proposed Classes, appointing Plaintiffs as class representative, and appointing their counsel to represent the Classes;

B. Awarding declaratory and other equitable relief as is necessary to protect the interests of Plaintiffs and the Class;

C. Awarding injunctive relief as is necessary to protect the interests of Plaintiffs and the Class;

D. Enjoining Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII;

E. Awarding Plaintiffs and the Class damages that include applicable compensatory, exemplary, punitive damages, and statutory damages, as allowed by law;

F. Awarding restitution and damages to Plaintiffs and the Class in an amount to be determined at trial;

G. Awarding attorneys' fees and costs, as allowed by law;

H. Awarding prejudgment and post-judgment interest, as provided by law;

I. Granting Plaintiffs and the Class leave to amend this complaint to conform to the evidence produced at trial; and

J. Granting such other or further relief as may be appropriate under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: November 30, 2023

Respectfully submitted,

s/ Lynn A. Toops
Lynn A. Toops (No. 26386-49)
Amina A. Thomas (No. 34451-49)
COHEN & MALAD, LLP
One Indiana Square, Suite 1400
Indianapolis, IN 46204
T: (317) 636-6481
F: (317) 636-2593
ltoops@cohenandmalad.com
athomas@cohenandmalad.com

Vicki J. Maniatis, Esq.
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN PLLC
100 Garden City Plaza, Suite 500
Garden City, New York 11530
Phone: (865) 412-2700
vmaniatis@milberg.com

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
5335 Wisconsin Ave., NW, Suite 440
Washington, DC 20015

Phone: 866.252.0878
dlietz@milberg.com

*Pro Hac Vice Application Forthcoming

Counsel for Plaintiffs and the Proposed Class